Feith Document Database v7
By Feith Software and Systems, Inc.

Feith Document Database Summary Report

The Joint Interoperability Test Command tested Feith Document Database (FDD) v7, a stand-alone records management application (RMA), at the Feith facility in Ft. Washington, PA from 17 through 21 November 2003. JITC Testers verified the implementation using version 7.1 of the Test Procedures for Chapters 2 (Baseline conformance) and 4 (Classified Records). FDD was compliant with DOD 5015.2-STD, dated 19 June 2002. All mandatory requirements were satisfied.

TABLE OF CONTENTS

1. Product Identification

Feith Document Database (FDD) v7 is a stand-alone records management application.

The Feith Document Database software package, as tested, consisted of the following component programs and utilities:

- Feith Document Database (FDD) v7 (used for filing, searching, and retrieving records)
- Feith MS Office Integrator (used to file records from MS Office applications)
- Feith Control Panel (FCP) (used for system/records management administration)
- FDD Auditor (used for audit administration)
- Feith Workflow iQ (used for retention schedule administration)

2. Test Configuration

The test configuration consisted of:

- One server running the Microsoft (MS) Windows 2000 Advanced Server operating system, Oracle 9i, Feith Mass Storage Server (EDStor), Feith Rules Engine (REX), Feith Page Exporter (FPX), Feith Page Remover (FDDPGRM), and Feith RMA Engine (RMAX).
- One server running Send Mail v8.11.6.
- One client personal computer (PC) running MS Windows 2000 Professional, Feith Document Database (FDD), MS Office 2000, Feith Control Panel (FCP), FDD Auditor, and Feith Workflow iQ.
- One client PC running MS Windows 2000 Professional, FDD, MS Office 2000, FCP, and Feith Workflow iQ.

3. RMA Mandatory Requirements

3.1 Managing Records [C2.1.1.]

Feith Document Database v7, hereafter referred to as FDD, manages electronic, non-electronic, and e-mail records. It stores electronic records in its repository and maintains them in their original, native file format. Users maintain records stored on other media (e.g. paper, diskette, tape) by adding a placeholder document and metadata through the user interface.

3.2 Accommodating Dates and Date Logic [C2.1.2.]

FDD stores and displays dates using a 4-digit year format, and recognize leap years including the year 2000. It accepts user input of valid dates from current, previous, and future centuries.

3.3 Implementing Standard Data [C2.1.3.]

FDD provides the capability to implement standardized data. Records managers can configure FDD with all the data elements as defined in DoD 5015.2-STD and additional fields for custom use. The additional fields can consist of text, date, or numeric fields.

3.4 Backward Compatibility [C2.1.4.]

As this is the first test of FDD against the new standard, no data was available to test backwards compatibility.[1]

3.5 Accessibility [C2.1.5.]

Feith provided the 508 Voluntary Product Accessibility Templates (VPATS) provided as Appendix C in the detailed test report.

3.6 Implementing File Plans [C2.2.1.]

Authorized users create file plan categories using the File Plan Manager within the Feith Control Panel (FCP). Authorized users specify category, disposition, event, and vital record information. Authorized users create disposition instruction workflows in the Feith Workflow iQ Manager to trigger disposition actions on record categories.

3.7 Scheduling Records [C2.2.2.]

FDD provides the capability to schedule any record by assigning a file code with an associated disposition based on a time period, a specified event, or both time and event. Record lifecycles are implemented through retention workflows.

3.8 Declaring and Filing Records [C2.2.3.]

FDD provides three methods for filing electronic records: the FDD interface, the Feith MS Office Integration, and MS Windows Explorer. FDD assigns a unique record identifier and a date/time stamp to each record. The date/time stamp serves as the required Date Filed field. Users cannot modify either field.

---

[1] Backward Compatibility is a new requirement in the June 2002 version of DoD 5015.2-STD.

3.9 Filing E-mail Records [C2.2.4.]

FDD provides the capability to file e-mail messages from MS Outlook 2000. It automatically captures message transmission and receipt data to populate the Subject or Title, Publication Date, Date Received, Author/Originator, Addressee(s), and Other Addressee(s) record profile fields. The Publication Date and Date Received fields are editable in the record profile but not on the e-mail itself. The email profile screen is the same as the electronic record profile screen.

FDD saves e-mail messages and attachments as one record with one record profile. Users have the option to save the attachments to their hard drive and filing as electronic records.

3.10 Storing Records [C2.2.5.]

FDD uses EDStor for storing and preserving electronic records. The permissions granted at the file cabinet level determine who has access to the records and what they can do with those records. Only users with appropriate access can delete records from the repository either through disposition processing or by deleting the record from the file cabinet.

3.11 Screening Records [C2.2.6.1.]

Records managers perform screening functions using the Feith Workflow iQ Manager. In the Workflow Manager, authorized users select a record category (referred to as file cabinets in FDD) to see how many records and/or folders are active within the specific workflow. Workflows can be configured with business logic so that the records manager receives an e-mail whenever a record or folder enters a specific task in the workflow.

3.12 Closing Record Folders [C2.2.6.2.]

FDD provides authorized users the ability to close folders through the Modify File Cabinet screen in the main FDD interface by entering the event, event and event date, or the cutoff date. Authorized users also have the option of modifying access permissions to the folder to prevent further filing by applying the "Closed" state to the folder.

3.13 Cutting Off Record Folders [C2.2.6.3.]

Authorized users cut off record folders using the Work to Do screen in the FDD interface. Authorized users select the Work to Do option from the Search menu in the main FDD interface. In the Work to Do screen, users select an Approve Cut Off task to view a listing of record folders ready for cut off and then select the record folder to submit it for cut off.

3.14 Freezing/Unfreezing Records [C2.2.6.4.]

FDD provides the capability for authorized users to freeze/unfreeze a record or folder through the FDD interface. The authorized user selects a record category and selects a record or folder. After selecting a record or folder, the user right clicks on the record or folder and applies or removes the "Frozen" state. An optional freeze reason may be assigned.

3.15 Transferring Records [C2.2.6.5.]

FDD provides the capability for authorized users to transfer records/folders through the Work to Do screen in the FDD interface. Authorized users select the Work to Do option from the Search menu in the main FDD interface. In the Work to Do screen, users select an Approve Transfer task to view a listing of record folders ready for transfer and then select the record folder to submit it for transfer.

3.16 Destroying Records [C2.2.6.6.]

FDD provides authorized users the ability to destroy records through the Work to Do Screen in the FDD interface. Authorized users select the Work to Do option from the Search menu in the main FDD interface. In the Work to Do screen, users select an Approve Destroy task to view a listing of record folders ready for destruction and then select the record folder to submit it for destruction.

3.17 Cycling Vital Records [C2.2.6.7.]

FDD provides authorized users the ability to cycle vital records through the Work to Do in the FDD interface. Authorized users select the Work to Do option from the Search menu in the main FDD interface. In the Work to Do screen, users select the Vital Review to view a listing of record folders ready for vital review and then select the record folder to submit it to be cycled.

3.18 Searching for and Retrieving Records [C2.2.6.8.]

FDD provides search and retrieve capabilities through the Search File Cabinet screen in the main FDD user interface. Users can search across all file cabinets or limit their search to a specific file cabinet. Users may retrieve a selected record and save it to their hard drive.

3.19 Access Control [C2.2.7.]

FDD has two types of access control permissions. Functional permissions define what FDD tasks a user or group can perform (e.g. filing, searching, deleting, or printing). Resource permissions control what FDD resources (e.g. filing or searching into a specific record category) a user or group can access; these permissions are assigned at the record category level. Additional record-level access restrictions were implemented using Supplemental Markings and the user-defined Project Name fields.

3.20 System Audits [C2.2.8.]

FDD provides the required system auditing capabilities through the FDD Auditor. Administrators control access to the FDD Auditor module by the limiting the installation of FDD Auditor to those users who require auditing capabilities.

3.21 System Management Requirements [C2.2.9.]

MS Windows 2000 Advanced Server and the Oracle 9i database management systems provided the required system management capabilities.

4. Non-Mandatory Features Demonstrated

4.1 Document Imaging Tools [C3.2.6.]

Feith Document Database (FDD) offers an object repository that stores scanned images, faxes, application files, e-mails, videos, etc. These objects are either key indexed or automatically indexed using recognition technology, such as bar-code and OCR, into one of several industry standard databases. Objects can be displayed in FDD either natively (.txt, .tif or .jpeg) or through in-place activation (OLE), depending on file type.

4.2 Workflow and/or Document Management Features [C3.2.11.]

Feith Workflow iQ provides a non-programmer workflow development environment supported by a graphical design, rules-based flow manager. Features, such as expected documents, load balancing, vital statistics, e-mail work-o-grams and auditing, provide the distribution, monitoring and control of the workflow process. Workflow iQ manages the retention workflow of records and folders.

5 Management of Classified Records

FDD was configured to satisfy all Chapter 4 requirements. The following paragraphs highlight FDD's implementation of specific Chapter 4 requirements.

5.1 Managing Classified Records [C4.1.]

FDD provides the capability to manage classified records as an extension of the baseline FDD system. Users can define custom fields to describe the classified record and file it to the EDStor repository.

5.2 Mandatory Metadata [C4.1.1.]

FDD can be configured to provide all the classified metadata elements as specified in Table C4.T1. of the Standard.

5.3 Classification Guides [C4.1.10.]

FDD implements classification guides as look ups. Users mouse right click on the field to display a menu with the Classification Guide option. Selecting that option allows users to select a guide and guide entry to apply. FDD copies the information from the guide entry into the relevant fields of the filing grid.

5.4 Editing Records [C4.1.12.]

Authorized users can search for classified records due for downgrade or declassification. If the classification status of the record changes, authorized users are allowed to edit the classified record metadata.

5.5 Restricted Data and Formerly Restricted Data [C4.1.13.]

FDD provides the capability to handle classified records with the "Restricted Data" and "Formerly Restricted Data" supplemental markings. When a user selects either marking, any data in the "Downgrade On" and "Declassify On" fields will not be saved, and FDD displays a warning message to the user.

5.6 Record History Audit [C4.1.16.]

FDD record history audit captures replaced metadata values, and the user who entered that value. Users can view, copy, save, and print the audit log based on their access permissions. The capability to delete the audit log is reserved for authorized users only.

5.7 Access Control [C4.1.20.]

FDD provides the capability to restrict access to records and their metadata based on access criteria. Users are assigned a classification (security) level of Top Secret, Secret, Confidential, or Unclassified. Security levels are hierarchical, therefore, those users assigned a "Secret" security level will only see documents marked Secret and below.

Users are also assigned supplemental markings. Supplemental markings do not override a user's access, but work in conjunction with the user's designated classification level to partition access. Additionally, FDD has the ability to restrict access on user-defined fields.

Last Updated: 22 January 2004